

# On the power quantum computation over real Hilbert spaces

Matthew McKague  
 Centre for Quantum Technologies  
 National University of Singapore  
 matthew.mckague@nus.edu.sg

September 6, 2011

## Abstract

We consider the power of various quantum complexity classes with the restriction that states and operators are defined over a real, rather than complex, Hilbert space. It is well known that a quantum circuit over the complex numbers can be transformed into a quantum circuit over the real numbers with the addition of a single qubit. This implies that BQP retains its power when restricted to using states and operations over the reals. We show that the same is true for QMA( $k$ ), QIP( $k$ ), QMIP, and QSZK.

## 1 Introduction

The standard quantum formalism specifies a complex Hilbert space, but one could just as well consider a real Hilbert space. In fact, a quantum formalism based on real Hilbert spaces has the same descriptive power as complex quantum formalism: given any description of a physical system using complex quantum formalism, there is a simple mapping to a description using real quantum formalism that gives the same predicted outcome statistics. Moreover, this description respects the division into subsystems [MMG09]. This means, for example, that there can be no experiment that can rule out real quantum formalism.<sup>1</sup>

Now let us consider computation. Does the choice of real or complex Hilbert spaces change the power of various computing models? At first it might seem that this is obvious: if any quantum system can be described using real Hilbert spaces, then why not the physical systems underlying some computing model? For computing models where all parties are trusted this is indeed the case. BQP, EQP and related classes are all unchanged as well as classes where messages are classical, such as QCMA.

However, for interactive proofs, where the prover(s) are not trusted, there are three important problems. First, in the case of two or more subsystems the mapping from complex to real descriptions introduces entanglement not present in the original complex description. This is problematic for classes like QMA(2) which does not allow provers to be entangled. Second, the mapping from complex to real descriptions does not preserve inner products. Hence states can become more distinguishable, which is problematic for classes like QSZK where certain states are required to be indistinguishable from others. Finally,

---

<sup>1</sup>Unless one makes assumptions about the dimension of systems.

the mapping to real descriptions is not onto. Hence untrusted parties may have access to a larger set of operations than in the original complex description.

## 1.1 Contributions

For any quantum complexity class let us define a restricted class such that all states and operators are defined over the real numbers instead of the complex numbers. We name these classes by adding a subscript  $\mathbb{R}$ . Thus BQP restricted to real gates and states becomes  $\text{BQP}_{\mathbb{R}}$ , etc.. We prove the following theorem:

**Theorem 1.**

$$\text{QMA} = \text{QMA}_{\mathbb{R}} \quad (1)$$

$$\text{QMA}(2) = \text{QMA}_{\mathbb{R}}(2) \quad (2)$$

$$\text{QIP}(k) = \text{QIP}_{\mathbb{R}}(k) \quad (3)$$

$$\text{QMIP}[m, k] = \text{QMIP}_{\mathbb{R}}[m, k + 1] \quad (4)$$

$$\text{QMIP}_{\text{ne}}[m, k] = \text{QMIP}_{\text{ne}\mathbb{R}}[m, k + m] \quad (5)$$

$$\text{QSZK} = \text{QSZK}_{\mathbb{R}}. \quad (6)$$

In order to prove this result we must overcome the difficulties mentioned in the introduction. The basic tool is an argument used in [MM11] to argue about security. The idea is this: in a certain basis the mapped description of a complex quantum state to a real quantum state looks like a coherent mixture of the original state and its complex state, identified by an extra qubit:

$$V |\psi'\rangle = \frac{1}{\sqrt{2}} |0\rangle |\psi\rangle + \frac{1}{\sqrt{2}} |1\rangle |\psi^*\rangle \quad (7)$$

where  $V$  is the change of basis matrix. Operators are similarly mapped:

$$VM'V^\dagger = |0\rangle\langle 0| \otimes M + |1\rangle\langle 1| \otimes M^*. \quad (8)$$

In this basis all the real operations of an honest party (the verifier, for example) commute with measuring the “extra” qubit in the  $Z$  basis. Hence we can reduce to a situation where we first measure to determine whether to perform original operations or complex conjugate operations, and then proceed. In either case the honest party has the same power, and susceptibility to being cheated, as in the original complex protocol.

We use this argument in two ways. First, we use it to show that we can transform a complex protocol into a real protocol and retain the same completeness and soundness. This applies to all the complexity classes we consider. Second, in a multi-party setting, if one party is honest then the other party cannot distinguish between states any more than in the original protocol. We use this when arguing about QSZK.

The remaining tool that we use is an argument that when a multi-party computation is separable then entanglement is not required in the real simulation. We then use a recent result [HM10] showing that  $\text{QMA}(2)$  can be restricted to separable operations. This allows us to argue successfully in the case of  $\text{QMA}(2)$ .

## 2 Real simulation

In this section we recall the relevant work on real simulation of arbitrary quantum systems over complex Hilbert spaces. In particular, we recall the real simulation of quantum circuits and multi-party computations. Importantly, we do not use the most obvious derivation, but use a different derivation which is conducive to our later arguments about computational complexity. We also consider another context for real simulation, where there is a multi-subsystem computation which is separable.

### 2.1 Single party

It is a well known result that any quantum circuit can be simulated over a real Hilbert space by using one additional qubit. The basic idea is to store the 2-dimensional real vector space represented by a complex number in a 2-dimensional real vector space corresponding to the additional qubit added to the circuit. It is quite easy to derive the transformation needed to take states and gates over a complex Hilbert spaces to states and gates over real Hilbert space. Here we will use a somewhat non-obvious derivation that will be helpful later. This derivation is based on that of [MM11].

Consider a state  $|\psi\rangle$  on some complex Hilbert space. We may operate on it using some unitary gate  $U$  and finally measure it according to some Hermitian observable  $M$ , obtaining an expected value  $\langle\psi|U^\dagger MU|\psi\rangle$ . We obtain the same expected value if we complex conjugate  $|\psi\rangle$ ,  $U$  and  $M$ :

$$\langle\psi|U^\dagger MU|\psi\rangle = \langle\psi^*|U^T M^* U^*|\psi^*\rangle. \quad (9)$$

Now suppose that we take a coherent mixture of the original circuit and its complex conjugate. That is, we start with a state

$$\alpha|0\rangle|\psi\rangle + \beta|1\rangle|\psi^*\rangle \quad (10)$$

where  $\alpha^2 + \beta^2 = 1$  and  $\alpha, \beta \in \mathbb{R}$ , then transform by the unitary

$$|0\rangle\langle 0| \otimes U + |1\rangle\langle 1| \otimes U^* \quad (11)$$

and measure with the Hermitian observable

$$|0\rangle\langle 0| \otimes M + |1\rangle\langle 1| \otimes M^*. \quad (12)$$

Then we again obtain the same expected value:

$$\alpha^2 \langle\psi|U^\dagger MU|\psi\rangle + \beta^2 \langle\psi^*|U^T M^* U^*|\psi^*\rangle = \langle\psi|U^\dagger MU|\psi\rangle. \quad (13)$$

Now we have the following idea: since the imaginary part of the complex conjugate is opposite the imaginary part of the original, we might be able to arrange  $\alpha$  and  $\beta$  so that the imaginary parts of the complex conjugate cancel those of the original, and we are left with something real. However the “extra” qubit gets in the way and it does not work out that way, but after a suitable change of basis we get something similar. We need  $\alpha = \beta = \frac{1}{\sqrt{2}}$  and the qubit unitary

$$V = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix}. \quad (14)$$

Then we find

$$\begin{aligned}\frac{1}{\sqrt{2}}V \otimes I (|0\rangle|\psi\rangle + |1\rangle|\psi^*\rangle) &= V\frac{|0\rangle + |1\rangle}{\sqrt{2}}\text{Re}|\psi\rangle + iV\frac{|0\rangle - |1\rangle}{\sqrt{2}}\text{Im}|\psi\rangle \\ &= |0\rangle\text{Re}(|\psi\rangle) + |1\rangle\text{Im}(|\psi\rangle).\end{aligned}$$

This is the usual state we obtain if we represent the complex amplitudes  $a + ib$  in  $|\psi\rangle$  with the real qubit  $a|0\rangle + b|1\rangle$ . Thus we may understand the real simulation of a quantum circuit as a coherent mixture of the original circuit and its complex conjugate, under a suitable change of basis.

Let us define the transformation  $R$  which takes complex states to real states (with double the dimension) as above:

$$R(|\psi\rangle) = |0\rangle\text{Re}|\psi\rangle + |1\rangle\text{Im}|\psi\rangle. \quad (15)$$

We define  $R(\langle\psi|)$  analogously, and  $R$  applied to operators by

$$\begin{aligned}R(M) &= V(|0\rangle\langle 0| \otimes M + |1\rangle\langle 1| \otimes M^*)V^\dagger \\ &= V(I \otimes \text{Re}(M) + iZ \otimes \text{Im}(M))V^\dagger \\ &= I \otimes \text{Re}(M) + iY \otimes \text{Im}(M) \\ &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \text{Re}(M) + \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \otimes \text{Im}(M).\end{aligned}$$

where the third line follows from the observation that  $VZV^\dagger = Y$ .

We obtain the following properties of  $R(\cdot)$ .

**Lemma 1.** *Let  $M, N$  be linear operators over a Hilbert space  $\mathcal{H}$ . Further, let  $|\psi\rangle \in \mathcal{H}$ . Then*

$$(V^\dagger \otimes I)R(M)(V \otimes I) = |0\rangle\langle 0| \otimes M + |1\rangle\langle 1| \otimes M^* \quad (16)$$

$$V^\dagger R(|\psi\rangle) = \frac{1}{\sqrt{2}}|0\rangle|\psi\rangle + \frac{1}{\sqrt{2}}|1\rangle|\psi^*\rangle \quad (17)$$

$$R(MN) = R(M)R(N) \quad (18)$$

$$R(M|\psi\rangle) = R(M)R(|\psi\rangle) \quad (19)$$

$$R(\langle\psi|)R(M)R(|\psi\rangle) = \text{Re}\langle\psi|M|\psi\rangle \quad (20)$$

*Also,  $R(M)$  is unitary (Hermitian, positive semi-definite) if and only if  $M$  is unitary (Hermitian, positive semi-definite).*

The first two lines are from the definition. The third and fourth line, and the last claim, are seen easily by undoing the change of basis by  $V$  and looking at the formulation in terms of the original and complex conjugate operators and vectors. The fifth line is obtained by the fact that the inner product is an equal mixture of the original and complex conjugate inner products, and hence only the real part remains.

## 2.2 Multiple parties

Suppose that we have some computation that happens between multiple parties and we wish to simulate the computation over real numbers instead of complex. Furthermore, we need the simulation to respect the original division into multiple parties. This can be accomplished by communicating the “extra” qubit between the parties, but this may not be feasible, for example in a Bell test. However, we can do the following: give a “copy” of the “extra” qubit to each party. When viewed as a coherent mixture of the original and complex conjugate computations this is immediately obvious. The state  $|\psi\rangle$  becomes

$$\frac{1}{\sqrt{2}}|00\dots 0\rangle|\psi\rangle + \frac{1}{\sqrt{2}}|11\dots 1\rangle|\psi^*\rangle \quad (21)$$

with one of the “extra” qubits given to each party. An operator  $M$  applied by the  $j$ th party becomes

$$|0\rangle\langle 0|_j \otimes M + |1\rangle\langle 1|_j \otimes M^* \quad (22)$$

where the subscript  $j$  indicates the  $j$ th “extra” qubit. Essentially, each party looks at their “extra” qubit to decide whether to apply the original or complex conjugate operator. Since the “extra” qubits are all correlated in the  $Z$  basis all the parties are coordinated.

Interestingly, if we apply  $V$  as in the previous section to each of the “extra” qubits, we obtain a real state. We refer the reader to [McK10] section 2.5.4 for the details of this calculation.

We define a new transformation  $R^{(m)}(\cdot)$  by

$$R^{(m)}(|\psi\rangle) = V_1 \otimes \dots \otimes V_m \left( \frac{1}{\sqrt{2}}|00\dots 0\rangle|\psi\rangle + \frac{1}{\sqrt{2}}|11\dots 1\rangle|\psi^*\rangle \right) \quad (23)$$

where there are  $m$  “extra” qubits, and analogously for  $R^{(m)}(\langle\psi|)$ . For operators we define  $R_j^{(m)}(\cdot)$  by

$$R_j^{(m)}(M) = |0\rangle\langle 0|_j \otimes M + |1\rangle\langle 1|_j \otimes M^* \quad (24)$$

We obtain the following properties of  $R^{(m)}(\cdot)$ .

**Lemma 2.** *Let  $M, N$  be linear operators over a Hilbert space  $\mathcal{H}$  and  $j, k \in \{1, \dots, m\}$ . Further, let  $|\psi\rangle \in \mathcal{H}$ . Then*

$$V_j^\dagger R_j^{(m)}(M) V_j = |0\rangle\langle 0|_j \otimes M + |1\rangle\langle 1|_j \otimes M^* \quad (25)$$

$$V_1^\dagger \otimes \dots \otimes V_m R^{(m)}(|\psi\rangle) = \frac{1}{\sqrt{2}}|0\dots 0\rangle|\psi\rangle + \frac{1}{\sqrt{2}}|1\dots 1\rangle|\psi^*\rangle \quad (26)$$

$$R^{(m)}(MN|\psi\rangle) = R_j^{(m)}(M) R_k^{(m)}(N) R^{(m)}(|\psi\rangle) \quad (27)$$

$$R^{(m)}(\langle\psi|) R_j^{(m)}(M) R^{(m)}(|\psi\rangle) = \text{Re} \langle\psi| M |\psi\rangle \quad (28)$$

$R_j^{(m)}(M)$  is unitary (Hermitian, positive semi-definite) if and only if  $M$  is unitary (Hermitian, positive semi-definite).

### 2.3 Separable states and operations

Suppose that we have a computation with multiple subsystems which is separable. That is, the state and operators can all be written in the form

$$M = \sum_j M_{1,j} \otimes \cdots \otimes M_{m,j} \quad (29)$$

where each  $M_{k,j}$  is Hermitian and operates on the  $k$ th subsystem only (Hence  $M$  is also Hermitian.)

To simulate general multi-partite computations the construction given in section 2.2 is required, and in particular this means that the state will be entangled across subsystems. In the case we are currently considering, we wish to maintain the separability. Fortunately, this is possible.

We will use the same methodology as in the previous sections, by considering coherent mixtures of the original and complex conjugate computation. For separable operators we can add an additional layer of complexity by considering a type of “partial” complex conjugation. The structure of the separable operator allows us to complex conjugate on only one subsystem in a well defined way. In the case of many subsystems, we can conjugate on a subset which we specify by way of a bit-string, which is the characteristic vector for the subset on which we conjugate:

**Definition 1** (Partial complex conjugation). *Let  $M = \sum_j M_{1,j} \otimes \cdots \otimes M_{m,j}$  be a separable operator. Then*

$$M^{*k} = \sum_j M_{1,j} \otimes \cdots \otimes M_{k,j}^* \otimes \cdots \otimes M_{m,j}. \quad (30)$$

*Let  $|\psi\rangle = |\psi_1\rangle \cdots |\psi_m\rangle$  be a product state. Then*

$$|\psi\rangle^{*j} = |\psi_1\rangle \cdots |\psi_j\rangle^* \cdots |\psi_m\rangle. \quad (31)$$

*Further, define  $M^{*z}$  for  $z \in \{0,1\}^m$  to be  $M$  with  $(\cdot)^{*k}$  applied for each  $k$  such that  $z_k = 1$  (Note that the order does not matter) and analogously for  $|\psi\rangle^{*z}$ .*

Just as the complex conjugate computation gives the same outcome statistics as the original computation, partial complex conjugation also preserves statistics.

**Lemma 3.** *Let  $M = \sum_j M_{1,j} \otimes \cdots \otimes M_{m,j}$  and  $N = \sum_k N_{1,k} \otimes \cdots \otimes N_{m,k}$  be separable operators. Then*

$$\text{Tr}(MN) = \text{Tr}(M^{*z}N^{*z}) \quad (32)$$

*for all  $z \in \{0,1\}^m$ .*

*Proof.* Note that it suffices to show  $\text{Tr}(MN) = \text{Tr}(M^{*t}N^{*t})$  for  $t \in \{1, \dots, m\}$  since we may apply induction to obtain the full result. As well, it suffices to show the result for  $m = 2$  and  $t = 1$  since we may permute systems and combine  $m - 1$  of the systems into 1 to reduce to this case.

$$\text{Tr}(MN) = \text{Tr} \left( \sum_{j,k} M_{1,j} \otimes M_{2,j} N_{1,k} \otimes N_{2,k} \right) \quad (33)$$

$$= \sum_{j,k} \text{Tr}(M_{1,j} N_{1,k}) \text{Tr}(M_{2,j} N_{2,k}) \quad (34)$$

$$= \sum_{j,k} \text{Tr}(M_{1,j} N_{1,k})^* \text{Tr}(M_{2,j} N_{2,k}) \quad (35)$$

$$= \sum_{j,k} \text{Tr}((M_{1,j})^* (N_{1,k})^*) \text{Tr}(M_{2,j} N_{2,k}) \quad (36)$$

$$= \text{Tr} \left( \sum_{j,k} (M_{1,j})^* \otimes M_{2,j} (N_{1,k})^* \otimes N_{2,k} \right) \quad (37)$$

$$= \text{Tr}(M^{*1} N^{*1}). \quad (38)$$

Here the third line follows from the fact that  $M_{1,j}$  and  $N_{1,k}$  are Hermitian.  $\square$

We are now ready to define the real simulation for a separable computation. We will consider the case of two subsystems, but the same techniques generalize for any number of subsystems. Also, we will only consider a measurement, but arbitrary separable super-operators can also be considered.

We begin with a product state  $|\psi\rangle = |\psi_1\rangle |\psi_2\rangle$  and a separable measurement  $M = \sum_j M_{1,k} \otimes M_{2,j}$ . Consider the state

$$|\psi'\rangle = \frac{1}{2} \sum_z |z\rangle_{1,2} |\psi\rangle^{*z} \quad (39)$$

and the operator

$$M' = \sum_{z \in \{0,1\}^2} |z\rangle\langle z|_{1,2} \otimes M^{*z}. \quad (40)$$

Note that  $|\psi'\rangle$  is a product state since it can be written (after permuting registers) as

$$\frac{1}{2} (|0\rangle_1 |\psi_1\rangle + |1\rangle_2 |\psi_1\rangle^*) (|0\rangle_2 |\psi_2\rangle + |1\rangle_2 |\psi_2\rangle^*) \quad (41)$$

and  $M'$  is separable.

Now let us evaluate  $\text{Tr}(|\psi'\rangle\langle\psi'| M')$ . First define  $\Pi_z = |z\rangle\langle z|_{1,2}$  to be the projection on to the computational basis state  $|z\rangle$  on the “extra” qubits. Then  $\sum_z \Pi_z M' \Pi_z = M'$  and hence

$$\text{Tr}(|\psi'\rangle\langle\psi'| M') = \sum_z \text{Tr}(|\psi'\rangle\langle\psi'| \Pi_z M' \Pi_z) \quad (42)$$

$$= \sum_z \text{Tr}((\Pi_z |\psi'\rangle\langle\psi'| \Pi_z) (\Pi_z M' \Pi_z)) \quad (43)$$

$$= \sum_z \text{Tr}(|\psi\rangle\langle\psi|^{*z} M^{*z}) \quad (44)$$

Lemma 3 applied for each  $z$  then gives

$$\text{Tr}(|\psi'\rangle\langle\psi'| M') = \text{Tr}(|\psi\rangle\langle\psi| M) \quad (45)$$

Now we apply the same trick as for the other real simulations, and perform a change of basis by  $V$  on each “extra” qubit to obtain real states and operators. Thus we make the following definitions:

$$\begin{aligned} R_{1,2}^{(2)}(|\psi_1\rangle|\psi_2\rangle) &= R_1^{(2)}(|\psi_1\rangle) \otimes R_2^{(2)}(|\psi_2\rangle) \\ &= V_1 \frac{1}{2} (|0\rangle|\psi_1\rangle + |1\rangle|\psi_1^*\rangle) V_2 (|0\rangle|\psi_2\rangle + |1\rangle|\psi_2^*\rangle) \end{aligned}$$

Here  $R_1^{(2)}$  and  $R_2^{(2)}$  are both just  $R$  as in section 2.1, but with different “extra” qubits. For operators we define

$$R_{1,2}^{(2)}(M) = \sum_j R_1^{(2)}(M_{1,j}) \otimes R_2^{(2)}(M_{2,j}) \quad (46)$$

$$= (V_1 \otimes V_2) \left( \sum_{z \in \{0,1\}^2} |z\rangle\langle z|_{1,2} \otimes M^{*z} \right) (V_1^\dagger \otimes V_2^\dagger). \quad (47)$$

We obtain the following properties:

**Lemma 4.** *Let  $M$  be a separable operator over a Hilbert space  $\mathcal{H}$ . Further, let  $|\psi\rangle = |\psi_1\rangle|\psi_2\rangle \in \mathcal{H}$ . Then*

$$\sum_{z \in \{0,1\}^2} |z\rangle\langle z|_{1,2} \otimes M^{*z} = (V_1^\dagger \otimes V_2^\dagger) R_{1,2}^{(m)}(M) (V_1 \otimes V_2) \quad (48)$$

$$V_1^\dagger \otimes V_2 R_{1,2}^{(2)}(|\psi\rangle) = \frac{1}{2} (|0\rangle|\psi_1\rangle + |1\rangle|\psi_1^*\rangle) (|0\rangle|\psi_2\rangle + |1\rangle|\psi_2^*\rangle) \quad (49)$$

$$\langle\psi|M|\psi\rangle = R_{1,2}^{(2)}(\langle\psi|) R_{1,2}^{(2)}(M) R_{1,2}^{(2)}(|\psi\rangle) \quad (50)$$

### 3 Complexity implications

The real simulation for single systems and lemma 1 immediately imply that  $\text{BQP} = \text{BQP}_{\mathbb{R}}$ ,  $\text{EQP} = \text{EQP}_{\mathbb{R}}$  and  $\text{QCMA} = \text{QCMA}_{\mathbb{R}}$ . We show that the analogous results are also true for  $\text{QMA}$ ,  $\text{QMA}(2)$ ,  $\text{QIP}$ ,  $\text{MQIP}$  and  $\text{QSZK}$ .

#### 3.1 $\text{QMA} = \text{QMA}_{\mathbb{R}}$

Suppose we have a problem in  $\text{QMA}$  with a verifier  $A(x)$ , which we model as a POVM element corresponding to “ACCEPT” for input  $x$ . That is, when the prover sends state  $|\psi\rangle$ , the verifier accepts with probability  $\langle\psi|A(x)|\psi\rangle$ . We suppose that  $A(x)$  has completeness  $c$  and soundness  $s$ . It is clear that  $R(\langle\psi|)R(A(x))R(|\psi\rangle) = \langle\psi|A(x)|\psi\rangle \geq c$ . Hence we obtain a real verifier that accepts valid real proofs with the same probability as the original verifier accepts valid proofs. In particular, the prover prepares  $R(|\psi\rangle)$  and sends it along to the verifier, complete with the “extra” qubit, since the prover no longer needs it.



Now consider an invalid real proof  $|\phi\rangle$  sent to the real verifier  $R(A(x))$ . Note that, with a dishonest prover, we do not yet know<sup>2</sup> if  $|\phi\rangle = R(|\psi\rangle)$  for any  $|\psi\rangle$  so we must work a little harder than in the honest prover case. However, recall that there is a unitary transformation  $V$  such that

$$V^\dagger R(A(x)) V = |0\rangle\langle 0| \otimes A(x) + |1\rangle\langle 1| \otimes A^*(x). \quad (51)$$

Thus measuring  $VZV^\dagger$  on the “extra” qubit commutes with  $R(A(x))$ . Since the qubit is then discarded we may assume that this measurement happens, and in particular that the prover does so. Hence the prover might as well have sent a mixture of  $V|0\rangle|\psi_0\rangle$  and  $V|1\rangle|\psi_1\rangle$  for some complex  $|\psi_0\rangle$  and  $|\psi_1\rangle$ . Note that the resulting mixture need not be real, but this only increases the power of the cheating prover. The probability of accepting is then a convex combination of  $\langle\psi_0|A(x)|\psi_0\rangle$  and  $\langle\psi_1|A^*(x)|\psi_1\rangle$ . Since these are both at most  $s$ , the overall acceptance probability is at most  $s$ . Hence  $R(A(x))$  is a verifier with the same completeness and soundness as  $A(x)$ . Thus we have proved that  $\text{QMA} = \text{QMA}_{\mathbb{R}}$ .

### 3.2 $\text{QMA}(2) = \text{QMA}_{\mathbb{R}}(2)$

We first recall a recent result of Harrow and Montanaro [HM10]. They prove that  $\text{QMA}(k) = \text{QMA}^{\text{SEP}}(2)$ . Here  $\text{QMA}^{\text{SEP}}(k)$  is the same as  $\text{QMA}(k)$  except that the “ACCEPT” POVM element  $A(x)$  is separable. Recall from the definition of  $\text{QMA}(k)$  that the provers must send unentangled states. Thus we are in the situation described in section 2.3.

Now suppose we have a problem in  $\text{QMA}(k)$ . We use Harrow and Montanaro’s construction to obtain a problem in  $\text{QMA}^{\text{SEP}}(2)$  with verifier separable  $A(x)$ , again modelled as the “ACCEPT” operator, which has completeness  $c$  and soundness  $s$ . Suppose there exists a valid proof  $|\psi_1\rangle|\psi_2\rangle$ . Then prover 1 can send  $R_1^{(2)}(|\psi_1\rangle)$  while prover 2 can send  $R_2^{(2)}(|\psi_2\rangle)$ . Meanwhile, the verifier becomes  $R_{1,2}^{(2)}(A(x))$  since it is separable. We then have

$$R_1^{(2)}(|\psi_1\rangle) R_2^{(2)}(|\psi_2\rangle) R_{1,2}^{(2)}(A(x)) R_1^{(2)}(|\psi_1\rangle) R_2^{(2)}(|\psi_2\rangle) = \langle\psi_1|\langle\psi_2|A(x)|\psi_1\rangle|\psi_2\rangle \geq c. \quad (52)$$

To analyze soundness we use an argument analogous to the  $\text{QMA}$  case. Suppose that some  $x$  is not in the language, so  $\langle\psi|A(x)|\psi\rangle \leq s$  for all  $|\psi\rangle$ . First we note that there exist unitaries  $V_1$  and  $V_2$  such that

$$V_1^\dagger \otimes V_2^\dagger R_{1,2}^{(2)}(A(x)) V_1 \otimes V_2 = \sum_{z \in \{0,1\}^2} |z\rangle\langle z| \otimes A(x)^{*z} \quad (53)$$

where  $|z\rangle$  is a computational basis state on the two provers’ “extra” qubits. Thus measuring  $V_1^\dagger Z V_1$  on prover 1’s “extra” qubit commutes with  $R_{1,2}^{(2)}(A(x))$  and we may assume that this happens, and in particular that prover 1 does so. Similarly, we may assume that prover 2 measures their “extra” qubit in the basis  $V_2^\dagger Z V_2$ . Hence the provers might as well have sent a mixture of  $V_1|j\rangle|\psi_j\rangle V_2|k\rangle|\phi_k\rangle$  for  $j, k \in \{0,1\}$  and for some complex  $|\psi_j\rangle$  and  $|\phi_k\rangle$ .

---

<sup>2</sup> In fact, this is always true for this situation, but we instead use the same argument that we use later for other situations.

Note that the resulting mixture need not be real, but this only increases the power of the cheating prover. The probability of accepting is then a convex combination of the form

$$\sum_{z \in \{0,1\}^2} p_z \langle \psi_{z_1} | \langle \phi_{z_2} | A^{*z}(x) | \psi_{z_1} \rangle | \phi_{z_2} \rangle. \quad (54)$$

By lemma 3 and the soundness of  $A(x)$ , each  $\langle \psi_{z_1} | \langle \phi_{z_2} | A^{*z}(x) | \psi_{z_1} \rangle | \phi_{z_2} \rangle$  is at most  $s$  and hence the overall acceptance probability is at most  $s$ . Thus  $R_{1,2}^{(2)}(A(x))$  is a verifier with the same completeness and soundness as  $A(x)$  and we have proved that  $\text{QMA}^{\text{SEP}}(2) = \text{QMA}(2)_{\mathbb{R}}$  and by extension  $\text{QMA}(2) = \text{QMA}(2)_{\mathbb{R}}$ .

We should point out that, unlike the proof for QMA here we are not allowed to simulate just any protocol for a QMA( $k$ ) problem. It must first be transformed into  $\text{QMA}^{\text{SEP}}(2)$  protocol before the mapping to a real protocol is applied.

### 3.3 QIP( $k$ ) = QIP $_{\mathbb{R}}$ ( $k$ )

First we argue that this result is indeed interesting. Since it is known that  $\text{QIP} = \text{IP}$  [JJUW10], it is trivially true that  $\text{QIP}_{\mathbb{R}} = \text{QIP}$ . However, since the  $\text{QIP} \subseteq \text{IP}$  inclusion is shown by proving that  $\text{QIP} \subseteq \text{PSPACE}$  there is not necessarily a relationship between the number of messages in a QIP protocol and the corresponding IP protocol. Indeed, a constant number of messages is not sufficient for IP unless  $\text{AM} = \text{PH}$ . Hence our result that  $\text{QIP}(k) = \text{QIP}_{\mathbb{R}}(k)$  is stronger than what can be derived from the fact that  $\text{QIP} = \text{IP}$ .

As for the proof, the situation for QIP is somewhat more complicated than for QMA since the prover and verifier must both perform computations, thus they must establish a shared pair of entangled “extra” qubits. However, a similar argument applies. We sketch the details.

Suppose we have a verifier  $A(x)$  for some problem in QIP( $k$ ) for  $k$  even. The verifier operates by preparing some initial state  $|0\rangle$  and applying some unitary  $U_1(x)$ . Then the verifier sends a portion of the state to the prover, keeping the rest in memory. After receiving a reply from the prover, the verifier applies  $U_2(x)$ . Continuing thus for some number of messages, the verifier finally measures according to  $M(x)$  and either accepts or rejects.

We can convert the entire procedure into a real quantum protocol as follows: the verifier prepares  $R^{(2)}(|0\rangle)$  which has two “extra” qubits. Then the verifier applies the unitary  $R_1^{(2)}(U_1(x))$  and sends the second “extra” qubit to the prover along with some portion of the remaining state, as in the original protocol. Note that the verifier sends this “extra” qubit on the first round only. The prover may use this “extra” qubit to perform operations, which are the prover’s original operations transformed by  $R_2^{(2)}(\cdot)$ . After each pair of messages, the verifier applies  $R_1^{(2)}(U_k(x))$  and finally measures according to  $R_1^{(2)}(M(x))$ .

It is easy to see that this real quantum protocol has the same completeness as the original protocol by appealing to lemma 2. For soundness we may apply an argument which analogous to that for QMA. We perform a change basis by  $V_1 \otimes V_2$  and find that, from the verifier’s perspective, the entire protocol is a coherent mixture of the original protocol and its complex conjugate. We next note that (in this basis) measuring the first “extra” qubit (held by the verifier) in the  $Z$  basis commutes with all subsequent operations.

Thus the verifier might as well have flipped a coin and chose whether to perform the original protocol or the complex conjugate, announcing to the prover which one was chosen (hence the second “extra” qubit). Clearly in either case the soundness is identical to the original protocol, and hence the soundness of the real quantum protocol is also identical to the original protocol.

For the case of  $\text{QIP}(k)$  with  $k$  odd we use a similar argument. Instead, however, the prover prepares the “extra” qubits and sends one to the verifier along with the initial message. Completeness is straightforward. For soundness we slightly modify the argument. Instead of the verifier choosing whether to perform the original protocol or the complex conjugate, the prover chooses.

Thus we have shown that  $\text{QIP}(k) = \text{QIP}_{\mathbb{R}}(k)$ .

One might wonder whether the multiparty real simulation is necessary: since the verifier and prover take turns they could communicate a single “extra” qubit back and forth. In fact, this is not sufficient. In the appendix we give an explicit example where the soundness of such a construction is not the same as in the original protocol.

### 3.4 $\text{QMIP}[m, k] = \text{QMIP}_{\mathbb{R}}[m, k + 1]$

The argument here is essentially the same as for  $\text{QIP}(k)$ , except that we need to make sure that all the provers are able to perform operations. This is accomplished as follows. Since the provers are allowed prior entanglement, they may share an entangled set of  $m+1$  “extra” qubits, and one prover entangles an additional qubit to send to the verifier along with the first message. If the original protocol had the verifier sending the first message then one of the provers sends an additional message at the beginning of the protocol containing just the “extra” qubit. This increases the number of messages by at most one.

If the provers are not allowed prior entanglement, as in  $\text{QMIP}_{\text{ne}}$ , then a different protocol is required. Here the verifier first prepares  $m + 1$  “extra” and sends  $m$  of them to the  $m$  provers as the first  $m$  messages, keeping one behind. This increases the number of messages by at most  $m$ .<sup>3</sup>

The arguments for soundness and completeness are by now predictable. The verifier’s actions, in a suitable basis, look like a coherent mixture of the original protocol and the complex conjugate. Thus we may assume that either the provers together choose which version the verifier should perform, or the verifier chooses and announces this choice to the provers. Both the original and complex conjugate protocols have the same soundness so the real quantum protocol also has the same soundness. Thus we have shown  $\text{QMIP}[m, k] = \text{QMIP}_{\mathbb{R}}[m, k + 1]$  and  $\text{QMIP}_{\text{ne}}[m, k] = \text{QMIP}_{\text{ne}\mathbb{R}}[m, k + m]$

### 3.5 QSZK

QSZK is essentially QIP with the additional restriction that, assuming an honest prover, at each step the verifier’s state must be close (in trace distance) to the output of an efficient quantum circuit (after tracing out non-output qubits.) We need only show that the verifier’s state is always close to the output of some efficient quantum circuit (assuming an honest prover).

---

<sup>3</sup>With a little thought this can be reduced to  $m - 1$  in general and further for particular protocols.

Let  $P$  be the honest prover for some protocol. Then  $P'$  is the honest prover for the corresponding real protocol, where the operations of  $P'$  are those of  $P$ , transformed by  $R_2^{(2)}(\cdot)$ . Suppose that a dishonest verifier  $V'$  can use  $P'$  as a subroutine to produce a state that  $V'$  could not create efficiently alone. For our purposes we do not restrict  $V'$  to real operations, noting that this only increases  $V'$ 's power.

We now use the usual argument, but applied to  $P'$  rather than the verifier. In a suitable basis  $P'$ 's operations commute with measuring  $P'$ 's “extra” qubit, and hence  $P'$ 's actions look like either those of the original prover  $P$  or the complex conjugate  $P^*$ . We first suppose that  $V'$  prepares the prover's “extra” qubit. Then the verifier can either produce some state  $\rho_0$ , by choosing that  $P'$  perform the original protocol, or some other state  $\rho_1$  by choosing that  $P'$  perform the complex conjugate protocol, or some mixture of  $\rho_0$  and  $\rho_1$ . Since we assume that the resulting state cannot be prepared by  $V'$  efficiently alone, either  $\rho_0$  or  $\rho_1$  must also have this property. But this contradicts the assumption that the original protocol (and by symmetry the complex conjugate protocol) is from QSZK. The case where  $P'$  prepares the “extra” qubit is similar, except the state produced is always  $\frac{1}{2}(\rho_0 + \rho_1)$ .

## 4 Conclusions

We have demonstrated that a wide variety of important quantum complexity classes are unchanged when the quantum operations are restricted to be over a real Hilbert space. The arguments that we use are quite general and could be applied to other complexity classes as well.

**Acknowledgements** This work is funded by the Centre for Quantum Technologies, which is funded by the Singapore Ministry of Education and the Singapore National Research Foundation. Thanks to Bill Rosgen for helpful discussions.

## References

- [HM10] Aram Harrow and Ashley Montanaro. An efficient test for product states, with applications to quantum merlin-arthur games. In *Foundations of Computer Science (FOCS), 2010*, pp. 633 – 642, January 2010. DOI:10.1109/FOCS.2010.66. EPRINT arXiv:1001.0017.
- [JJUW10] Rahul Jain, Zhengfeng Ji, Sarvagya Upadhyay, and John Watrous. Qip = pspace. In *Proceedings of the 42nd ACM symposium on Theory of computing, STOC '10*, pp. 573–582, New York, NY, USA, 2010. ACM. DOI:10.1145/1806689.1806768. EPRINT arXiv:0907.4737.
- [McK10] Matthew McKague. *Quantum Information Processing with Adversarial Devices*. PhD thesis, University of Waterloo, June 2010. EPRINT arXiv:1006.2352, URL <http://hdl.handle.net/10012/5259>.
- [MM11] Matthew McKague and Michele Mosca. Generalized self-testing and the security of the 6-state protocol. In Wim van Dam, Vivien Kendon, and Simone Severini, editors, *Theory of Quantum Computation, Communication, and Cryptography*,

*Lecture Notes in Computer Science*, volume 6519, pp. 113–130. Springer Berlin / Heidelberg, 2011. DOI:10.1007/978-3-642-18073-6\_10. EPRINT arXiv:1006.0150.

[MMG09] Matthew McKague, Michele Mosca, and Nicolas Gisin. Simulating quantum systems using real hilbert spaces. *Physical Review Letters*, **102**(2):020505, 2009. DOI:10.1103/PhysRevLett.102.020505. EPRINT arXiv:0810.1923.

[Wat02] John Watrous. Limits on the power of quantum statistical zero-knowledge. In *Proceedings. The 43rd Annual IEEE Symposium on Foundations of Computer Science, FOCS 2002*, pp. 459 – 468, February 2002. DOI:10.1109/SFCS.2002.1181970. EPRINT arXiv:quant-ph/0202111.

## A The single party real simulation is not sufficient to show $\text{QIP}(k) = \text{QIP}_{\mathbb{R}}(k)$ .

Suppose we make the following argument: the prover and verifier take turns performing operations, so we really only need one “extra” qubit, and they can pass it back and forth along with the messages. We can thus transform the states and all operations according to  $R(\cdot)$ . Clearly the completeness is the same, but what about soundness? Here we give an example problem with an instance not in the language where in the original protocol the verifier accepts with probability arbitrarily close to 0, but for the real simulation with only one “extra” qubit there is a cheating prover that forces verifier to always accept.

The problem we consider is quantum state distinguishability. This is a complete problem for the class QSZK [Wat02]. We are given two efficient quantum circuits  $Q_0$  and  $Q_1$  that produce outputs  $\rho_1$  and  $\rho_2$  after tracing out non-output qubits, and the promise that either

$$\|\rho_1 - \rho_2\|_1 \leq \alpha \tag{55}$$

or

$$\|\rho_1 - \rho_2\|_1 \geq \beta \tag{56}$$

with  $\alpha, \beta \in [0, 1]$  and  $\alpha < \beta^2$ . The problem is to determine which of these is true. The basic solution to this problem is to prepare one of  $\rho_0$  or  $\rho_1$  at random and send it to the verifier. The prover attempts to decide which state was sent, and sends a guess to the verifier. The verifier then checks whether the prover was correct. If the prover is very often correct over many instances of this game, then the states must be far apart in the trace norm and the verifier accepts. If the states are close together then the prover will be correct about half of the time and the verifier rejects.<sup>4</sup>

Now we consider two unitaries  $U_0$  and  $U_1$  which differ only in their global phase. In particular,  $U_0|0\dots 0\rangle = iU_1|0\dots 0\rangle$ . Clearly the two states must be completely indistinguishable since  $\rho_0 = \rho_1$ . However, if we apply the real simulation and pass the “extra”

---

<sup>4</sup> A more sophisticated argument involves first amplifying to obtain a pair of circuits with  $\alpha$  close to 0 and  $\beta$  close to 1 and then playing the game once. Then completeness is close 1, soundness is close to  $\frac{1}{2}$  and only two messages are required. See Watrous [Wat02] for details.

qubit to the prover, the states are orthogonal and the prover can distinguish them perfectly! Indeed, according to lemma 1

$$\begin{aligned}
R(\langle 0 \dots 0 | U_0^\dagger) R(U_1 | 0 \dots 0) &= \langle 0 \dots 0 | U_0^\dagger U_1 | 0 \dots 0 \rangle \\
&= \operatorname{Re} i \\
&= 0.
\end{aligned}$$

A closer inspection reveals that  $R(U_0 | 0 \dots 0) = (X \otimes I) R(U_1 | 0 \dots 0)$ . Thus the prover needs only to measure the “extra” qubit in the  $Z$  basis to distinguish the states. The reason that the previous proof fails for this construction is that the prover’s measurement on the “extra” qubit does not commute with measurement in the  $V^\dagger Z V$  basis, so we can no longer view the verifier’s actions as a mixture of the original and complex conjugate protocols (they share the “extra” qubit). In the construction with two “extra” qubits the verifier keeps one qubit, so *all* operations, both the verifier’s and the prover’s, commute with measurement in the  $V^\dagger Z V$  basis.